Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	DA 18-783
Wireless Telecommunications Bureau and	)	
Office of Engineering and Technology	)	
establish procedure and deadline for filing	)	
Spectrum Access System initial commercial	)	GN Docket No. 15-319
deployment proposals	)	
	)	

To: Marlene H. Dortch

Office of the Secretary, Federal Communications Commission

APPLICATION OF FAIRSPECTRUM LLC FOR SHORT-TERM, LIMITED GEOGRAPHIC COMMERCIAL DEPLOYMENT IN THE 3550-3700 MHZ BAND

In response to the above-mentioned Public Notice (notice)[1] from the Wireless Telecommunications Bureau and the Office of Engineering and Technology issued on July 27, 2018, Fairspectrum LLC, a wholly owned U.S. subsidiary of Fairspectrum Oy, Finland, hereby submits its proposal for a short-term, limited geographic commercial deployment (Initial Commercial Deployment or ICD) in the 3550-3700 MHz band (3.5 GHz Band).

Heikki Kokkinen
Chief Executive Officer
Fairspectrum LLC

Fairspectrum is pleased to offer its proposal for ICD. Fairspectrum compliments the Commission for its pioneer work in the area of Dynamic Spectrum Access and for the enabled possibilities of new consumer and business communication services in the band.

[1] See The Wireless Telecommunications Bureau (WTB) and the Office of Engineering and Technology (OET) (collectively, WTB/OET) of the Federal Communications Commission (Commission or FCC) seek proposals for short-term, limited geographic commercial deployment (Initial Commercial Deployment or ICD) by conditionally approved Spectrum Access System (SAS) Administrator(s) in the 3550-3700 MHz band (3.5 GHz Band), as directed by the *3.5 GHz First Report & Order*.

Table of contents

Table of contents **2**

Abbreviations **4**

1 User registration process **7**

2 SAS-CBSD Communications **10**

2.1 Commercial partners of Fairspectrum 14

3 Professional Installation **14**

4 SAS-SAS Interoperability **15**

5 SAS Utilization of Commission Databases **16**

6 DPA Protection **18**

7 Incumbent Protection Implementation **19**

7.1 Propagation model 19
7.2 Federal incumbent protection 21
7.3 PAL protection 22
7.4 FSS and GWBL protection 23
7.5 ESC protection 25
7.5 Incumbent presence simulation 25

8 Interference Reports and Mitigation **26**

9 Description of testing scenarios **28**

9.1 SAS-CBSD Interface tests 28
9.1.1 CBSD Registration 28
9.1.2 CBSD Spectrum Inquiry 28
9.1.3 CBSD Spectrum Grant 29
9.1.4 CBSD Heartbeat 29
9.1.5 CBSD Measurement report 29
9.1.6 CBSD Spectrum Relinquish 29
9.1.7 CBSD Deregistration 29
9.1.8 CBSD Device Security Validation 29

9.1.9 CBSD Domain Proxy Security Validation 30
9.2 SAS-SAS Interface tests 30
9.2.1 SAS-SAS Security, Authentication, and Encryption Protocols 30
9.2.2 SAS-SAS Full Activity Dump Message 30
9.3 SAS Functional tests 30
9.3.1 Exclusion Zone Enforcement 30
9.3.2 Propagation model and antenna gain 30
9.3.3 PPA creation 30
9.3.4 Aggregate interference protection - Single Protected Entity 31
9.3.5 ESC protection (Possible option) 31
9.3.6 PPA protection 31
9.3.7 GWPZ protection 31
9.3.8 FSS protection 31
9.3.9 Federal incumbent protection 32
9.3.10 Incumbent protection - Multi constraint protection 32
9.3.11 SAS Federal government database update 32
9.3.12 SAS WINNF Database update 32
9.3.13 International border protection 32
9.3.14 Quiet Zone protection 33
9.4 Channel allocation 33
9.5 Coordinated incumbent protection 33
9.6 Coordinated PAL protection 33

10 Generated data 33

11 Access to the SAS and data 35

12 Technical verification, and 35

13 Description of report after the ICD period 36

References 40

Abbreviations

CBRS	Citizens Broadband Radio Service
CBSD	Citizens Broadband radio Service Device
CEO	Chief Executive Officer
C.F.R.	Code of Federal Regulations
CGI	CBSD Group Identifier
CPI	Certified Professional Installer
CRL	Certification Revocation List
DP	Domain Proxy
DPA	Dynamic Protection Area
DySPAN	Dynamic Spectrum Access Networks
EAS	Equipment Authorization System
eHata	extended Hata
ESC	Environmental Sensing Capability
EUD	End User Device
EZ	Exclusion Zone
FCC	Federal Communications Commission
FSS	Fixed-Satellite Service
GAA	General Authorized Access
GESC	Gain of ESC sensor antenna
GWBL	Grandfathered Wireless Broadband Licensees
GWPZ	Grandfathered Wireless Protection Zones
ICD	Initial Commercial Deployment
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization of Standardization
ITM	Irregular Terrain Model
ITS	Institute for Telecommunication Sciences
JSIR	Joint Spectrum Interference Resolution
JSON	JavaScript Object Notation
LLC	Limited Liability Company
LSA	Licensed Shared Access
LTE	Long Term Evolution
MA	Massachusetts
MDPA	Move list for Dynamic Protection Area
MRLC	Multi-Resolution Land Characteristics Consortium
NACP	Native American Cancer Prevention
NLCD	National Land Cover Database

NTIA	National Telecommunications and Information Administration
OET	Office of Engineering and Technology
OpenSSRF	Open source Standard Spectrum Resource Format
Oy	Osakeyhtiö (Limited Liability Company)
UR-ID	User Registration ID
PAL	Priority Access License
PKI	Public Key Infrastructure
PL	Path Loss
PPA	PAL Protection Area
PZ	Protection Zone
RFC	Request For Comments
RMS	Root Mean Square
SAS	Spectrum Access System
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
SSC	Spectrum Sharing Committee
TLS	Transport Layer Security
ULS	Universal Licensing System
US	The United States
U.S.C.	Code of Laws of the United States of America
WG	Working Group
WINNF	Wireless Innovation Forum
WTB	Wireless Telecommunications Bureau

Fairspectrum has applied to become a SAS Administrator in the second wave. Fairspectrum is committed to complete the two-stage review process. As a part of the second stage, Fairspectrum will complete the system testing in a controlled lab environment and wait for WTB/OET approval of successful laboratory test results, before conducting this ICD. Fairspectrum requests that this ICD would be considered as the public testing period and field trials for the final SAS Administrator certification.

The purpose of this document is to describe how Fairspectrum LLC demonstrates that its SAS complies with the Commission's rules, particularly those requirements and core functions described in Part 96, subpart F. This document contains the following further sections: 1 User registration process, 2 SAS-CBSD Communications, 3 Professional Installation, 4 SAS-SAS Interoperability, 5 SAS Utilization of Commission Databases, 6 DPA Protection, 7 Incumbent Protection Implementation, 8 Interference Reports and Mitigation, 9 Description of testing scenarios, 10 Generated data, 11 Access to the SAS and data, 12 Technical verification, and 13 Description of report after the ICD period. Each of these sections begin with a quote, which is marked with an italic font type, from the FCC notice. The quote refers to the information FCC requires in an ICD application and the further text with a normal font type describes Fairspectum's response to the requested information.

1 User registration process

A description of the process by which users can register with the SAS, receive authentication, and obtain user IDs during ICD.

Fairspectrum SAS has a pre-registration (enrollment) system for CBSD Users, who can be organizations or individuals. The user is a person or a company who owns and is responsible for one or more CBSDs. The user registration with Fairspectrum SAS is a manual process[2] via a Web User Interface. A user, who would like to begin to use Fairspectrum SAS service, makes a business contact with Fairspectrum by meeting in person or using phone, email, letter, text message, skype, Whatsapp, or similar methods.

[2] WINNF-15-S-0112 Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. Appendix A. V2.0.0. Feb 3, 2017.

Fairspectrum validates the user in the same way as any business partner by discussing, making a calls, sending emails, checking websites and social media, interviewing commonly known persons, checking IDs, or company registrations. When the business relationship is formed, the validity of the user is checked, for example, by comparing the company registration number to the official company registry, checking who has the right to sign on behalf of the organization based on the the articles of association stored in the official company register, and checking the identity of the signing person and the position of the person in the organization. In the signed agreement with the user, the user with rights to handle user data is named and the clauses to ensure correctness and avoid misuse of the CBRS system are confirmed. All CBSD user actions are authenticated, authorised, and access logs are stored. The technical compatibility is tested and verified before operation of the ICD SAS-licensee system. Fairspectrum creates a user account for the user and sends a one-time password to the user.

With the one-time password, the user can access the user page in the Fairspectrum SAS website. The Fairspectrum SAS website is secured using Transport Layer Security[3] (TLS) protocol. The user must change the password and in order to continue the user registration the user must fill in the following user registration information[4]: user legal identity, user mailing address (contact address), user's physical address, user's legal address, user's email contact address, and user's phone number. After the user has provided this necessary owner contact information, and accepted the part 96 license rules[5] and federal operations risks according to 96.55(e)[6] and FCC-15-47A1 paragraph 274[7], Fairspectrum SAS

[3] IETF RFC5246. The Transport Layer Security (TLS) Protocol. Version 1.2. Aug, 2008.
[4] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018.
[5] Title 47, Code of Federal Regulations, Part 96 (2015).
[6] Title 47, Code of Federal Regulations, Part 96.55 Information gathering and retention. (e) The SAS shall process and retain acknowledgements by all entities registering CBSDs that they understand the risk of possible interference from federal Incumbent User radar operations in the band.
[7] Federal Communications Commission, "Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band," GN Docket 12-354, FCC 15-47, Report and Order and Second Notice of Proposed Rulemaking, Released April 21, 2015. Paragraph 274 Consistent with NTIA's recommendation, Citizens Broadband Radio Service users will be required to accept interference – including potentially harmful interference – from federal radar systems as a condition of their authorization. We require Citizens Broadband Radio Service users to acknowledge that they understand and accept the risk of interference from federal radar systems. This requirement is consistent with the approach we adopted in the recent AWS-3 proceeding and will apply to all Citizens Broadband Radio Service users regardless of their area of operation or their status as a Priority Access Licensee or GAA user.599 Such acknowledgements may be made

provides the user with an User Registration Identity (UR-ID). The user registration process can be found in Figure 1.1.

During the User registration process and subsequent account maintenance, the Fairspectrum SAS records and maintains the following information with the registered user: User Registration date, User Registration expiration or term, User Registration state (valid, expired, pending enforcement, revoked), Registering Agent (FCC, SAS, or other agent), Optional Registration Fee Paid (true or false indication). A list of the CBSDs (CBSD-IDs) registered by the user.

Fairspectrum SAS has the possibility for the user and SAS Administrator to maintain an association of a CBSD with the CBSD User. Fairspectrum and the users use TLS protocol to identify the user securely and to establish the relationship between the CBSD and its user. The user information association is established per individual CBSD in such a way that CBSD users may revoke the CBSD's identity within the CBRS. The user has a possibility to create sub-groups of CBSDs.

With the user account in Fairspectrum SAS, the Registered User is able to: Update contact information, Update the list of fielded CBSDs by registering or deregistering CBSDs associated with a user account, Update information lists associated with that user account, including the following:

- Addition, deletion or administration of groupings of CBSDs (administer CGIs).
- Update the list of PPAs by means of the associated unique PPA-ID (administer PPAs).
- Addition, deletion or administration of groupings of registered PPAs.
- For each and every PPA, the PAL Holder is be able to update the list of CBSDs on that PPA's Cluster List.
- For each and every PPA, the PAL Holder is able to update the list of vertex points (boundary definitions) for that PPA.
- For each and every PPA, the PAL Holder may be able to query the SAS for the SAS calculated Largest Allowable Claim Contour.
- For each and every PPA, the PAL Holder may be able to query the SAS for the existing

through the SAS upon registering a CBSD. SAS Administrators must develop policies and procedures to ensure that such acknowledgements are properly recorded and maintained.

registered vertex points defining the PPA boundary.

- For each and every leased PPA, the PAL Holder is able to update the list of lessee claimed PPAs.
- The PAL Holder may be able to add, delete or administer groupings of Leased PPAs.
- For each and every leased PPA, the PAL Holder is able to update the list of CBSDs on that lessee's PPA's Cluster List.
- For each and every leased PPA, the PAL Holder is able to update the list of lessee's vertex points that define the boundary for that PPA.
- For each and every leased PPA, the PAL Holder is able to update the initiation and termination dates for that leased PPA.
- For each and every leased PPA, the PAL Holder is able to query the SAS for the existing SAS registered initiation and termination dates for that leased PPA.

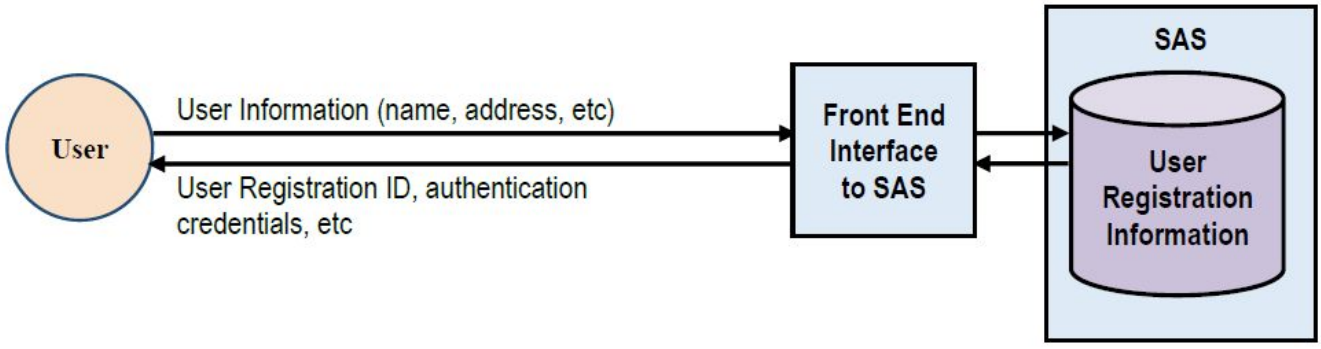

Figure 1.1. User Registration Process[8] (includes a secure mechanism for CBSD-Owner association)

2 SAS-CBSD Communications

The processes that the SAS will follow to communicate with and manage multiple CBSD and/or Domain Proxy (DP) products, including the protocols for SAS-CBSD communications for registration, channel grant, and channel release. Proposals should identify all commercial partners of the SAS Administrator.

[8] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018.

Fairspectrum registers, authenticates, and authorizes CBSDs. Before allowing an entity to register CBSDs, the entity needs to create a partnership with Fairspectrum. As part of the partnership, Fairspectrum or authorized CBRS certificate authority provide the partner with credentials, which are required to register CBSDs. The CBSD registration is carried out with Registration procedure of WINNF-TS-0016 or its latest version. Authentication is carried out with Authentication procedure of WINNF-TS-0016 or its latest version. The mutual authentication is based on Public Key Infrastructure and certificates (RFC-5280[9]) on TLS-v1.2 (RFC-5246[10]) following the WINNF-TS-0022[11] certificate policy. Fairspectrum follows the security recommendations in WINNF-TS-0065[12] or its latest version and WINNF-TS-0071[13] or its latest version. The authorization is based on §96.49. Fairspectrum utilizes the hooks for information verification and authorization provided by WINNF-TS-0247.[14] The content of the CBSD information is checked field by field to insure that it is correct type and within the limits of the allowed values. The blacklisted devices and users are checked before authorization. The communication between the Fairspectrum SAS and any other entity, including a CBSD, Domain Proxy, another SAS, and possibly with ESC, and all user interfaces is encrypted using TLS ciphersuites. The access to management interfaces is authenticated and authorized. Each user type has different authorization levels allowing access to respective information and capabilities. On organizational level, Fairspectrum applies Information Security controls of ISO/IEC 27001:2013(en)[15] and ISO/IEC 27002:2013(en).[16] For all FCC Identifiers intending to register, Fairspectrum checks the validity of the ID from the Commission's Equipment Authorization System[17] (EAS) and uses that

[9] RFC-5280. Internet X.509 Public Key Infrastructure Certificate and Certification Revocation List (CRL) Profile. Available at https://www.ietf.org/rfc/rfc5280.txt.
[10] RFC-5246. The Transport Layer Security (TLS) Protocol Version 1.2. Available at https://www.ietf.org/rfc/rfc5246.txt.
[11] WINNF-TS-0022 Version 1.1.2. CBRS PKI Certificate Policy. 6 February 2018.
[12] WINNF-TS-0065 Version 1.1.0. 26 July 2017. CBRS Communications Security Technical Specification..
[13] WINNF-TS-0071 Version 1.0.0. 26 July 2017. CBRS Operational Security Technical Specification.
[14] WINNF-TS-0247 V1.0.0 CBRS Certified Professional Installer Accreditation. 18 October 2017.
[15] ISO/IEC 27001:2013(en) Information technology. Security techniques. Information security management systems. Requirements.
[16] ISO/IEC 27002:2013(en) Information technology. Security techniques. Code of practice for information security controls.
[17] FCC EAS FCC Equipment Authorization System. Available at https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

information in authorization. Only registered and authenticated CBSDs are authorized to use the Fairspectrum SAS service.

When federal incumbents are protected with Protection Zones, Fairspectrum only authorizes CBSDs within the Protection Zones based on ESC information according to §96.67. Fairspectrum computes and utilizes PAL Protection Areas according to §96.25 and relevant WINNF specifications.

A Domain Proxy may represent a number of CBSDs according to WINNF-TS-0016[18] or its latest version. When Domain Proxy represents a number of CBSDs, TLS mutual authentication is carried out between the SAS and the Domain Proxy. A successful authentication is prerequisite for all SAS-CBSD and SAS - Domain Proxy procedures. If there is a Domain Proxy and the Domain Proxy is performing bulk CBSD registration, the Domain Proxy aggregates registration information for multiple CBSDs. The Domain Proxy sends an array of RegistrationRequest objects to the SAS which represents the aggregated CBSD registration information. Upon reception of the array of RegistrationRequest objects, the SAS initiates registration for each CBSD. The SAS responds with an array of RegistrationResponse objects, each containing a registration response to a CBSD. A Domain Proxy correlates the response objects with request objects using the JSON array object order. JSON arrays are ordered sequences; as such, a multiple request message or multiple response message contains an ordered sequence of objects. Domain Proxies, SASs and CBSDs preserve array ordering. SASs receiving a message having an array of request objects shall response with an array of response objects in which the order of the response objects is exactly matched to the order of the request objects.

The Fairspectrum SAS uses the WINNF-TS-0016 or its latest version, Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification. The architecture of the SAS-CBSD protocol can be found in Figure 2.1. A domain proxy can group messages of several CBSDs, which are administered by the domain proxy. From Internet client-server perspective, SAS is the server and domain proxy or CBSD is the client.

[18] WINNF-TS-0016 Version 1.2.1. 3 January 2018. Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification.

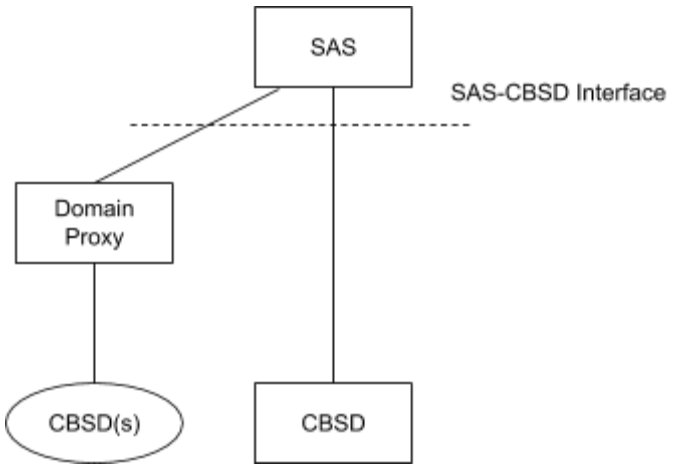

Figure 2.1. SAS-CBSD protocol architecture according to WINNF-TS-0016[64]

The 1.2.1 version (Jan 3, 2018) of the specification contains the following procedures: Pre-requisite procedures, SAS Discovery, Authentication, CBSD Registration, CBSD Spectrum Inquiry, CBSD Grant, CBSD Heartbeat, CBSD Grant Relinquishment, and CBSD Deregistration. The messages are encoded using JavaScript Object Notation (JSON) according to RFC-7159[19] and transported with TLS. Multiple data elements can be aggregated in a single request.

The CBSDs have to register with the Fairspectrum SAS and they have to provide installation details. The user, an authorized associate, or and employee of the user my install Category A CBSDs. The user installed CBSDs have to obtain the location and provide the location information to SAS as part of the CBSD registration. A certified professional installer only is allowed to install Category B devices. The certified professional installer can also install Category A devices. The Category A devices, which cannot determine the location automatically must be installed by a certified professional installer. The PAL License (PAL-ID) and specific PAL protection area (PPA-ID) have to be pre-registered in the SAS in the case of CBSDs using PAL spectrum.

2.1 Commercial partners of Fairspectrum

In ICD, Fairspectrum has at least one commercial partner of the following types: Network operator, CBSD Manufacturer, Another SAS provider, and possibly ESC Administrator.

[19] RFC-7159. The JavaScript Object Notation (JSON) Data Interchange Format.

3 Professional Installation

The process that a certified professional installer (CPI) would follow to register CBSDs/DPs during ICD and an explanation regarding how that professional installation will ensure the SAS can accurately locate devices in compliance with Part 96.

The CBSDs are installed by an employee of an operator or by a professional installer contracted by the operator. Fairspectrum requests from the operator the person name and the CPI certification of the person, who installs or has installed the CBSDs. Generally, the Fairspectrum process of verifying the installation information and persons carrying out the information are according to WINNF-TS-0247[20] or its latest version. Fairspectrum checks from the professional installer that he or she has CPI Certification. Fairspectrum gives access rights to the professional installer to configure the device information in Fairspectrum SAS. Fairspectrum SAS user interface has conditional clauses, which ensure that the information, which has to be filled is entered and they ensure that depending on the certification status of the installer and the device type only certain information can be configured. Alternatively, the certified professional installer can write the CBSD information on a paper and confirm the correctness with his or her signature. An employee of the operator or a Fairspectrum administrator can enter the written information of the certified professional installer in Fairspectrum SAS. If the data is not entered by the professional installer, Fairspectrum checks that the written information from the professional installer and the data entered into SAS are the same during ICD. Only after this process, a CBSD can begin automated channel allocation requests with the Fairspectrum SAS.

4 SAS-SAS Interoperability

An explanation regarding how the SAS Administrator will demonstrate its ability to correctly synchronize and exchange information with other SASs and correctly apply information security procedures and incumbent protection methods during ICD. For any SAS Administrator that does not

[20] WINNF-TS-0247 Version 1.0.0. 16 October 2017. CBRS Certified Professional Installer Accreditation Technical Specification.

plan to perform ICD with other SASs, it may describe how it will make a similar demonstration by simulating the presence of a separate SAS.

Fairspectrum has a business relationship with other SAS providers. When the business relationship is formed, the validity of the SAS provider is checked, for example, by comparing the company registration number to the official company registry, checking who has the right to sign on behalf of the organization based on the the articles of association stored in the official company register, checking the identity of the signing person and the position of the person. In the signed agreement with the SAS provider, the SAS provider person(s) with rights to handle SAS data is named and the clauses to ensure correctness and avoid misuse of the CBRS system are confirmed. After signing the agreement, the respective keys and certificates to enter, administer, and maintain SAS data are given to the agreed persons of the ESC provider. Fairspectrum checks from FCC that the SAS provider is authorized to operate a SAS service. All SAS provider actions are authenticated, authorised, and access logs are stored. The technical compatibility is tested and verified before operation of a production SAS-SAS system.

The Fairspectrum SAS uses the WINNF-TS-0096[21] or its latest version, Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - SAS Interface Technical Specification. The 1.3.0 version (24 April 2018) of the specification contains a SAS-SAS prerequisites: communication security, data use restrictions agreements, and peer SAS Discovery. The specified procedures include SAS mutual authentication and communications security based on TLS, record exchanges, and message flow. SAS-SAS synchronization contains time-range request support, By-ID request support, push support, and full record dump. Message encoding and transport are based on JSON and TLS. From Internet client-server perspective, each SAS operates as a server and as a client. The SAS is both able to make requests and respond to requests. The data can be carried both in request and in response, see Figure 14.2.

[21] WINNF-TS-0096 Version 1.2.0 SAS-SAS Protocol Specification. 22 October 2017.

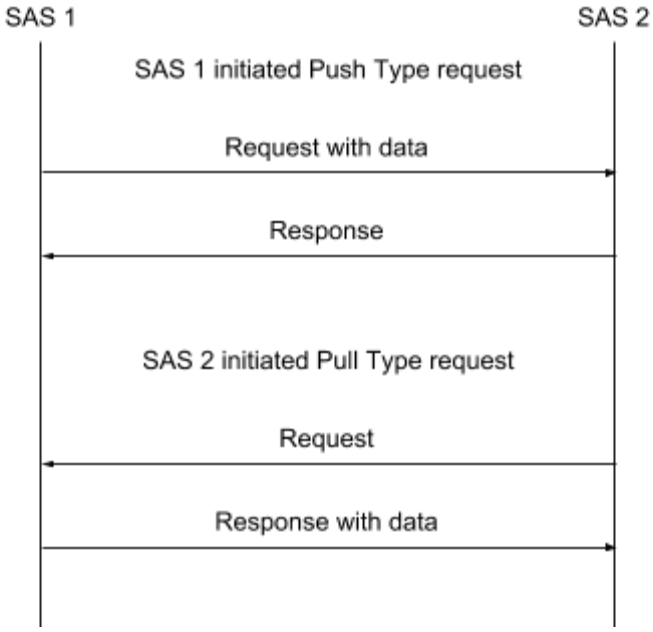

Figure 14.2. SAS-SAS message exchanges, data in request and response according to WINNF-TS-0096 [22]

The supported messages include: SAS Administrator, SAS Implementation, CBSD Data, Incumbent Protection Data, ESC Sensor, Zone Definition, Coordination Event, and Full Activity Dump. Fairspectrum will carry out the test and certification process as described in WINNF-TS-0061[23] or in its latest version. The current version 1.3.0 of Aug 21, 2018 contains the following functional tests: SAS-SAS security, authentication, and encryption protocols and SAS-SAS Full Activity Dump message.

5 SAS Utilization of Commission Databases

The processes that a SAS will follow to access, read, and use data directly from FCC databases during ICD, pending database availability.

Fairspectrum SAS will be technically capable of directly interfacing with any necessary FCC database containing information required for the proper operation of an SAS according to § 96.55. Those databases could include information for example about federal and non-federal incumbents like Fixed

[22] WINNF-TS-0096 Version 1.3.0 SAS-SAS Protocol Specification. 24 April 2018.
[23] WINNF-TS-0061 Version 1.3.0 Test and Certification Specification; SAS as Unit Under Test. 21 August 2018.

Satellite Service (FSS), Grandfathered Wireless Protection Zones (GWPZ), FCC field offices, or Priority Access Licences (PAL); certified CBRS entities and organizations like Spectrum Access Systems (SAS), Environmental Sensing Capability (ESC), Certified Professional Installers (CPI). Moreover, Fairspectrum SAS will use external data like Dynamic Protection Areas (DPA), Exclusion Zone (EZ) geographic and atmospheric information like country bordes, license areas, radio climate, refractive index, topography, and land clutter data.

Fairspectrum implements automatic download process which checks the changes in data availability and downloads automatically so that the latest data is always available in Fairspectrum SAS. The check and download periods are selected so that the delay requirements for a SAS Administrator are fulfilled. Fairspectrum keeps a record of timestamped downloaded datasets and time of use of specific datasets.

Fairspectrum automatically checks the conformance of the datasets and informs FCC immediately of the non-conformant data. Fairspectrum implements a human process to handle the non-conformant datasets, which may include verifying the cause of non-conformance, communication with FCC and other SAS Administrators, and correcting actions for the non-conformant data.

Fairspectrum obtains and stores data according to Commission Rule §96.55. Fairspectrum collects the registration information by utilizing registration procedure of WINNF-TS-0016[24] or its latest version. Fairspectrum keeps information on registered CBSDs according to Commission Rules §96.39, §96.43, and §96.45; geographic locations; protected Fixed Satellite Service (FSS) locations according to Rule §96.17; and, the Exclusion Zones and Protection Zones of the federal Incumbents.

Fairspectrum provides required CBSD coordination information to other SAS Administrators utilizing the protocol specified in WINNF-TS-0096 or its latest version. Fairspectrum provides CBSD registration information to general public so that identities are concealed. Fairspectrum stores the registration information and location of protected earth stations in database tables according to Rule §96.17. Fairspectrum stores the user transmission log files, excluding the federal users, for at least 60 months. Fairspectrum does not store federal Incumbent User information from ESC anymore than ESC approval policy dictates. Fairspectrum designs all required system integration work to interface with

[24] WINNF-TS-0016 Version 1.2.1 SAS to CBSD Protocol Specification. 3 January 2018.

FCC databases. Fairspectrum collects acknowledgements from all CBSD registering entities that they understand risk of possible interference from federal Incumbent radar operating in the band.

Fairspectrum SAS server processing environment has a software client, e.g. https client, sftp client, or scp client, which is configured with the selected authentication credentials, like shared secret, client certificate, or user name and password. The FCC database access client software has a timing mechanism implemented either in the client software itself or in the operating system e.g. as cron task. The timing mechanism is scheduled to synchronize with the FCC databases at least once a day. The FCC database access client software downloads the new files from the FCC database. It carries out a necessary amount of consistency checks about the data. If there are inconsistencies, the synchronization process is aborted and the system administrator is alerted to study the issues. Otherwise, the data on the SAS server is synchronized with the FCC database downloaded data. Depending on the type of data, pre-processing of the data may be carried out before it is taken into account in the SAS-CBSD communication.

6 DPA Protection

If a SAS Administrator intends to operate its SAS pursuant to the conditional waiver granted in the DPA Waiver Order, it must provide a declaration that its system will be DPA-enabled and a description of how it will demonstrate its ability to implement notification-based DPA protection using a portal.

Fairspectrum provides the DPA protection according to WINNF-TS-0112[25] or its latest version. At the time Fairspectrum SAS receives a notification from an ESC that a DPA needs protection, Fairspectrum SAS activates that DPA on the protected frequencies. The SAS monitors ESC operation failures, such failure could for example be communication connection break with an ESC. In the case of no connection to ESC, all DPAs are activated on all frequencies.

Fairspectrum SAS differentiates the protection of DPAs for Category A and B devices and in-band and out-of-band frequency ranges according to WINNF-TS-0112. For every protection constraint

[25] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018

Fairspectrum SAS determines the associated move list. Fairspectrum SAS determines the move list for protection area DPA on frequency range (MDPA) as a union of move list for all protection constraints, where the associated protection point is within the protection area DPA. Whenever any DP is activated on any given channel, Fairspectrum SAS for ensures that the CBSDs, which are under its management and which are members of the move list MDPA, are not transmitting using any grant that has a frequency range that overlaps with the channel ch from a time starting no later than 300 seconds after the activation of the DPA until no earlier than the time when the DPA becomes deactivated.

7 Incumbent Protection Implementation

The processes that a SAS Administrator will use to ensure the correct implementation of all relevant interference protection criteria, including how the SAS's over the air propagation testing will address the protection of Fixed Satellite Service (FSS) earth station sites, federal inland radar test sites, and area-based protections (e.g., Grandfathered Wireless Protection Zones). If the SAS Administrator does not expect the operation of one of these types of incumbents within the area it intends to serve during ICD, it should explain how it will make a similar demonstration by simulating the presence of that type of incumbent.

This section addresses the interference protection mechanisms to prevent harmful interference towards the incumbents and Priority Access Licensees. Fairspectrum SAS does not authorize operation of CBSDs within Protection Zones except as set forth in §96.15.

7.1 Propagation model

Fairspectrum SAS uses the propagation models as defined in WINNF-TS-0112[26] for calculating the PAL protection contours and aggregate interference on FSS, GWBL or ESC receiver. The selection of either ITM model in point-to-point mode[27] or extended Hata model (eHata)[28] depends on various

[26] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018.
[27] NTIA – ITS Irregular Terrain Model (ITM) (Longley-Rice) (20MHz-20 GHz): http://www.its.bldrdoc.gov/resources/radio-propagation-software/itm/itm.aspx
[28] NTIA. 3.5 GHz Exclusion Zone Analyses and Methodology Available at https://www.ntia.doc.gov/report/2015/35-ghz-exclusion-zone-analyses-and-methodology

conditions. For CBRS to incumbent receiver distances $d \leq 0.1$ km, the free-space path loss, as defined in WINNF-TS-0112, is used. For $0.1 < d < 1.0$ km, the eHata model without site-specific corrections is used. For $1.0 \leq d \leq 80.0$ km, the ITM model is used if the path loss using the ITM model using reliability and confidence factors of 0.5 is greater than the corresponding path loss using the eHata model. For $d > 80$ km, the ITM model is used. The distance d is calculated according to the methodology described in WINNF-TS-0112. The Vincenty's Inverse Solution is used to find the distance and azimuth (used in determining the antenna gains) between transmitter and receiver. The Vincenty's Forward Solution is used to find latitude and longitude coordinates along the propagation path. The coordinates, in turn, are used to query the terrain elevations from the Fairspectrum topographical database to be used in the path loss calculations.

Furthermore, if the CBRS effective antenna height, h_b, is greater than 200 m or if the clutter category, *r*, is "rural" at the location of the CBSD, the ITM model is used independent of the distance. For path lengths between the CBSD and victim receiver $d < 3$ km, h_b is the height of the CBSD, h_{cbsd}. For path lengths $3 \leq d \leq 15$ km, h_b is the CBSD antenna height h_{cbsd} + (d-3)/12 times the difference between the terrain elevation at the CBSD antenna and the average terrain elevation over a distance of 3 km to the location of the receiver. For $d > 15$ km, h_b is the CBSD antenna height h_{cbsd} + the difference between the terrain elevation at the CBSD and the average terrain elevation over the range 3 – 15 km. Moreover, h_b is restricted to be at least 20 m independent of the calculated effective receiver height.

These models have been adapted to the Fairspectrum SAS as an internal part of the software. Fairspectrum is open to WINNF suggestion per FCC approval on the used propagation model and will implement other models whenever proposed by the regulative and standardization bodies.

7.2 Federal incumbent protection

For federal Incumbent Users operating in band 3550-3650 MHz, the Fairspectrum SAS provides protection in the following way: CBSDs and End User devices (EUD) must not cause interference towards the federal Incumbent Users authorized to operate in the 3550-3700 MHz band and below 3550 MHz, and they must accept possible interference from Incumbent Users. For Category A CBSDs,

the Fairspectrum SAS will maintain up-to-date information about the EZs along the US coastline and around federal radiolocation sites using the NTIA data[29] as described in the section 5.1 CBRS architecture of this document. Exclusion Zone protection methodology is applied until one or more ESCs are approved, which effectively changes the protection type to Protection Zone. Fairspectrum SAS may authorize Category A CBSDs geographic areas outside the Exclusion Zones if all the other protection criteria are met and before ESC(s) are approved. Furthermore, once an ESC is approved and used by at least one SAS, the Fairspectrum SAS authorizes CBSD transmissions based on the information provided by an approved ESC. Category B CBSDs are only authorized when information about the federal incumbent use is present and provided to the Fairspectrum SAS by an approved ESC. Within no more than 300 seconds after the ESC has observed presence of an federal Incumbent User, the Fairspectrum SAS ensures that the CBSDs are suspended or moved to another frequency. Moreover, If the President of the United States or another Federal Government body instructs to discontinue the use of CBSDs, the Fairspectrum SAS instructs the CBSDs to cease all communication. Fairspectrum SAS will adapt to changes in the federal EZs and PZs to protect current or future federal Incumbent Users as requested by the FCC either on temporal or continuous basis.

For federal Incumbent Users operating in band 3650-3700 MHz, the Fairspectrum SAS provides protection in the following way: CBSDs and End User devices (EUD) must not cause interference towards the federal Incumbent Users authorized to operate in the 3550-3700 MHz band and below 3550 MHz, and must accept possible interference from Incumbent Users. The Fairspectrum SAS maintains up-to-date information about the EZs 80 km radius around the federal radiolocation sites listed in §90.133 and §2.106. Exclusion Zone protection methodology is applied until one or more ESCs are approved, which effectively changes the protection type to Protection Zone. The Fairspectrum SAS is consistent about the information of the presence of federal Incumbent User provided by an approved ESC, and enforces this information when authorizing the CBSD transmission within the PZ. Within no more than 300 seconds after the ESC has observed presence of an federal

[29] NTIA 3550-3650. NTIA. Spectrum Management. 3550-3650 MHz. Available at https://www.ntia.doc.gov/category/3550-3650-mhz.

Incumbent User, the Fairspectrum SAS ensures that the CBSDs are suspended or moved to another frequency. Moreover, If the President of the United States or another Federal Government body instructs to discontinue the use of CBSDs, the Fairspectrum SAS instructs the CBSDs to cease all communication.

7.3 PAL protection

The PAL licensees are auctioned by the FCC, where each PAL licensee is assigned to license area, which could be e.g. Partial Economic Areas or census tracts. Subsequently, the PALs are registered in the system and the Fairspectrum SAS verifies each individual PAL using the PAL-ID, User Registration Identity (UR-ID), FCC tract identity information (which license area is assigned to the PAL), and frequency channel logical identity information (which frequencies are auctioned to the PAL).

The Fairspectrum SAS provides PAL protection in the 3550-3650 MHz band by using the information of the PALs obtained from the FCC together with the relevant data. The data includes land clutter data and elevation data in order to calculate the PPA for both -96 dBm and -80 dBm contours. PAL licensees can also choose to report a PPA that is smaller in geographical area than the area calculated by the Fairspectrum SAS. The Fairspectrum SAS assigns each PAL to a license area and channel, as specified in section 1.3 Assigning frequencies of this document. The Fairspectrum SAS manages subsequent CBSD transmissions so that the aggregate interference of the GAA CBSDs within 40 km of the PPA is below -80 dBm/MHz for all points in the protection area.

The Area-Protection-Reference-Standard is described as follows: A fixed grid spanning candidate CBSD locations is defined. The grid has points separated by 2 arcseconds in north/south and east/west directions. The grid is aligned to integer latitude and longitude lines. The protection area is defined by a set of bounding contours. Protection points of a protection area are grid points of the fixed grid within the protection area. Protection to this area provided by a SAS ensures that estimated aggregate

interference falls below the predefined limit at each protection point. The aggregate interference calculations are performed assuming the use of an isotropic antenna integrating over a 10 MHz bandwidth and using a specified elevation above ground level.

As a result of a conservative SAS estimate, that aggregate interference from interfering CBSDs is expected to be less than or equal to a specified protection level for all protection points.

7.4 FSS and GWBL protection

"A description of how the SAS will ensure that non-federal FSS earth stations and grandfathered 3650-3700 MHz licensees are protected from harmful interference consistent with the rules."

Fairspectrum does not allow CBSDs to operate within areas that may cause interference to FSS earth station above the levels described in § 96.17(a) and (b), provided that the licensee of the FSS earth station and the authorized user of the CBSD mutually agree on such operation and the terms of any such agreement are provided to Fairspectrum according to § 96.17(e).

The Fairspectrum SAS provides incumbent protection in the 3650-3700 MHz band by using the information of the FSS and GWBL in the database together with the relevant data. The information includes land clutter data and elevation data, and the information about the CBSD making the request such as geolocation and transmit antenna configuration parameters. The purpose is to calculate the aggregate interference originated from the CBSDs located within 150 km for co-channel FSS, 40 km for adjacent channel FSS, and 40 km for Grandfathered Wireless Protection Zones (GWPZ), by using the propagation models as defined in section 7.1 Propagation model. The procedure for FSS operating in the 3600-3700 MHz is as follows:

1. Calculate the CBSD antenna gain towards the victim FSS receiver. This is obtained by determining the angle between the axis of the main beam of the CBSD towards the FSS receiver and the corresponding antenna gain using the radiation pattern reported by the CBSD. If the radiation pattern is not reported, the generic formula for the antenna gain given in WINNF-TS-0112[30] is used.

[30] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018.

2. Calculate the FSS antenna gain towards the CBSD. This is obtained by determining the angle between the axis of the main beam of the FSS towards the CBSD and the corresponding antenna gain using the radiation pattern reported by the FSS.
3. Calculate the path loss between the CBSD and FSS using the propagation model chosen with the criteria given in section 7.1 Propagation model. The calculation utilizes transmitter/receiver antenna height information, land clutter class at the location of the CBSD, and the elevation data along the propagation path.
4. Estimate the received aggregate interference level at the FSS receiver by taking into account the antenna gains as described above, the maximum EIRP reported by the CBSD in the registration or grant request, and signal losses. The root mean squared (RMS) of the aggregate interference of the CBSDs within 150 km from the FSS location is not permitted to exceed -129 dBm / MHz for co-channel, or -60 dBm for adjacent channel blocking CBSDs within 40 km from the FSS location. If the received interference power falls below these limits in the co/adjacent channels, the CBSD is permitted to transmit with the reported operational parameters.

Moreover, for protection calculations of FSS operating in the 3700-4200 (out-of-band), Fairspectrum uses an equivalent methodology and will ensure that aggregate interference of the CBSDs within 40 km stays below the predefined thresholds as given in WINNF-TS-0112.[31] FSS licensees operating in the 3600-3700 Mhz and in 3700-4200 MHz can also request for additional protection from Fairspectrum SAS through a dedicated informing interface build in the Fairspectrum SAS.

The protection of the existing GWBL operators in the 3650-3700 MHz corresponds to the methods presented for PAL and FSS. The GWBLs can operate within their GWPZ area. The aggregate interference from CBSDs within 40 km from the protection points, defined using the Area-Protection-Reference -Standard described in section 11.2 PAL protection, is then calculated using the methodology described in the four steps above, and shall not exceed -80 dBm/10 MHz in any point inside the GWPZ. Furthermore, the Fairspectrum SAS ensures that the GWBL shall not cause harmful

[31] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018.

interference to the existing grandfathered FSS earth stations operating in the 3650-3700 MHz, nor to the federal Incumbent Users until the last Grandfathered Wireless Broadband Licensee's license expires.

7.5 ESC protection

The Fairspectrum SAS provides ESC sensor protection as needed, optional depending on the availability of ESC during the Fairspectrum ICD. The ESC operator can require protection by providing the geolocation, antenna height, radiation pattern, antenna gain, and other relevant information from the sensor to Fairspectrum SAS, which then calculates the aggregate interference from all CBSDs within 40 km from the sensor location and manages the CBSD transmission so that the interference falls below 107 dBm/MHz – PL (Path Loss) + GESC, where GESC is the maximum gain of the ESC sensor antenna.

7.5 Incumbent presence simulation

If the SAS Administrator does not expect the operation of one of these types of incumbents within the area it intends to serve during ICD, it should explain how it will make a similar demonstration by simulating the presence of that type of incumbent.

Fairspectrum provides a web user interface for incumbents. With the user interface it is possible to create simulated same incumbents types with specific locations that are protected in CBRS system. The simulated incumbents cause the same protection procedures as the real incumbents in Fairspectrum SAS system. A difference to handling the simulated incumbents is that they are not communicated to other SAS Administrators systems and in the reports created by Fairspectrum SAS, they can be separated from real incumbents.

8 Interference Reports and Mitigation

A description of the SAS Administrator's proposed real-world interference mitigation demonstration and the performance of its reporting requirement. SAS Administrators should include details regarding whether its real-world testing will or will not include incumbents such as FSS licensees or federal

inland radar test sites.

Fairspectrum fulfills the requirements for SAS Administrator reporting in WINNF-TS-0112[32]. Fairspectrum publishes clearly the contact information where the Incumbent Access users can report interference and additional protection. In the case, these requests are received through other communication means, Fairspectrum employees copy the received information in the Fairspectrum interference reporting tools. The interference management tool sends a notification to Fairspectrum employees who are in shift to manage the interference issues so that they can be promptly addressed. The reports from the following organizations are handled with the highest priority: The Federal Government, Operators of incumbent Fixed-Satellite Earth Stations, Operators of incumbent Wireless Broadband Service stations operating in the 3650-3700 MHz band, Operators of networks protected by Priority Access licenses, Operators of network equipment licensed by GAA rules, Other SAS Administrators, and ESC Operators.

The reports are classified either by the person creating the report or by Fairspectrum employee to following groups: The report of erroneous data in the SAS database; The report of harmful interference experienced by an incumbent station or Priority Access licensee which is prohibited by Part 96 rules; The report of an alternative interference protection relationship between an incumbent user and CBSDs operating under Part 96 (e.g. an FSS user, see 96.17(e)); The report of an alternative interference protection relationship between a network operator protected by a Priority Access license and other CBSDs operating under Part 96 (see 96.41(d)(1)); The report by the FCC of an enforcement action, including any action taken regarding a particular CBSD or group of CBSDs or regarding a particular CBRS user or group of users; Information on waivers the FCC has granted to provide an exception to Part 96 rules for CBSDs or other CBRS entities; Information on waivers the FCC has granted to non-CBRS entities which impact CBRS operations; The request by an FSS earth station licensee pursuant to 47 CFR 96.17(f) for additional SAS protection of a licensed site.

When Fairspectrum receives such a report, Fairspectrum provides the full details of the report to all

[32] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018.

other SAS Administrators using coordination type formats INTERFERENCE_REPORT or ENFORCEMENT_ACTION of SAS-SAS protocol according to WINNF-TS-0096[33]. Reports originated by the Federal Government, reports of alternative interference protection relationships between incumbents and CBSDs or between Priority Access and General Authorized Access users are always provided to other SAS Administrators without delay. Reports leading to corrections in the SAS database shall be communicated to other SAS Administrators without delay insofar as the correction will impact previously-communicated information the SAS Administrator has corrected as a result of the report. Reports of harmful interference are by default communicated to other SAS Administrators in the process of responding to such a report. The tools provided by Fairspectrum for the reporting of harmful interference should provide sufficient information for the reporter of such harmful interference to follow standardized reporting procedures such as OpenSSRF formats and the JSIR process. Such tools also inform the user that reports may be acted upon by the FCC. Fairspectrum responds in a timely fashion corresponding to the nature of the report of exceptional circumstances, including those of harmful interference.

Fairspectrum supports the reporting requirements set in WINNF-TS-0096 or its latest version. Fairspectrum follows and implements the Wireless Innovation Forum SSC WG1 Exception Management Task Group recommendations how trouble tickets and exceptions are managed, including FCC input, reports from incumbents, and reports from PAL. Fairspectrum provides an interface for the FCC, incumbents including operators of FSS earth stations, grandfathered licenses, PALs, GAAs and administrators of other SAS and ESC. There is a free form available for reporting about possible interference incidents. The interference incident reports will be provided to other SAS administrators and to the FCC. Fairspectrum helps the FCC and other SAS administrators to identify the cause of interference, to solve the interference issue immediately, and to make any required changes to avoid such interference incidents in the future.

[33] WINNF-TS-0096. Spectrum Access System (SAS) - SAS Interface Technical Specification. Apr 24, 2018.

9 Description of testing scenarios

Each ICD Proposal must include detailed descriptions of the specific testing scenarios that the SAS Administrator intends to run during ICD, which may include operational parameters (e.g., the number, locations, and configuration of CBSDs).

In addition to the normal operation of SAS for its business purpose, Fairspectrum carries out the same test topics as in the laboratory testing[34] during ICD. The purpose of the test cases is to verify the same topics, but not necessarily exactly the same test cases. The testing cases are adapted to the ICD environment and a few of the test case, which are impractical in the ICD environment, are dropped out.

9.1 SAS-CBSD Interface tests

Test cases, which are not possible with the physical CBSDs, may be simulated with a software client acting as a CBSD.

9.1.1 CBSD Registration

This section provides the target of the testing scenario of SAS implementation of CBSD Registration Procedure. The test cases attempt to cover the following responses: 0 SUCCESS, 100 VERSION, 101 BLACKLISTED, 102 MISSING_PARAM, 103 INVALID_VALUE, 200 REG_PENDING.

9.1.2 CBSD Spectrum Inquiry

This section provides the target of the testing scenario of SAS Spectrum Inquiry Response to a CBSD Spectrum Inquiry Request. It assumes as a precondition that CBSD has successfully registered with the SAS and has obtained a cbsdId. The test cases attempt to cover the following responses: 0 SUCCESS, 101 BLACKLISTED, 102 MISSING_PARAM, 103 INVALID_VALUE, 300 UNSUPPORTED_SPECTRUM .

9.1.3 CBSD Spectrum Grant

This section provides the target of the testing scenario of SAS CBSD Grant Response to a CBSD Grant Request. The test cases attempt to cover the following responses: 0 SUCCESS, 101 BLACKLISTED,

[34] WINNF-TS-0061. V1.2.0. 6 June 2018. Conformance and Performance Test; SAS as Unit Under Test (UUT)

102 MISSING_PARAM, 103 INVALID_VALUE, 300 UNSUPPORTED_SPECTRUM, 400 INTERFERENCE, 401 GRANT_CONFLICT.

9.1.4 CBSD Heartbeat

This section provides the target of the testing scenario of SAS CBSD Heartbeat Response to a CBSD Heartbeat Request. The test cases attempt to cover the following responses: 0 SUCCESS, 100 VERSION, 101 BLACKLISTED, 102 MISSING_PARAM, 103 INVALID_VALUE, 500 TERMINATED_GRANT, 501 SUSPENDED_GRANT, 502 UNSYNC_OP_PARAM.

9.1.5 CBSD Measurement report

This section provides the target of the testing scenario of SAS CBSD Measurement Report Response to a CBSD Measurement Report Request. The test cases attempt to cover the following responses: 0 SUCCESS, 102 MISSING_PARAM, 103 INVALID_VALUE.

9.1.6 CBSD Spectrum Relinquish

This section provides the target of the testing scenario of SAS CBSD Spectrum Relinquish Response to a CBSD Spectrum Relinquish Request. The test cases attempt to cover the following responses: 0 SUCCESS, 100 VERSION, 102 MISSING_PARAM, 103 INVALID_VALUE.

9.1.7 CBSD Deregistration

This section provides the target of the testing scenario of SAS CBSD Deregistration Response to a CBSD Deregistration Request. The test cases attempt to cover the following responses: 0 SUCCESS, 102 MISSING_PARAM, 103 INVALID_VALUE.

9.1.8 CBSD Device Security Validation

This section provides the target of testing scenario of SAS validation of CBSD security credentials.

9.1.9 CBSD Domain Proxy Security Validation

This section provides the target of testing scenario of SAS validation of Domain Proxy security credentials.

9.2 SAS-SAS Interface tests

Test cases, which are not possible with another operational SAS, may be simulated with a software client acting as a SAS.

9.2.1 SAS-SAS Security, Authentication, and Encryption Protocols

This section provides the target of testing scenario of SAS validation of SAS security credentials.

9.2.2 SAS-SAS Full Activity Dump Message

This section provides the target of testing scenario of SAS validation of the Full Activity Dump exchange procedure.

9.3 SAS Functional tests

9.3.1 Exclusion Zone Enforcement

This section provides the target of testing scenario of the conformance of SAS implementation of the Exclusion Zone Enforcement.

9.3.2 Propagation model and antenna gain

This section provides the target of testing scenario of verifying that SAS correctly calculates:

1. path loss based on propagation models, and

2. the antenna gains of CBSDs and FSS based on locations and antenna patterns of the transmitter and the receiver.

9.3.3 PPA creation

This section provides the target of testing scenario of successful execution and completion of the PPA Creation.

9.3.4 Aggregate interference protection - Single Protected Entity

This section provides the target of testing scenario for SAS to authorize CBSDs to transmit only when they do not interfere with a protected entity. The scope of this test is to verify that the SAS continuously maintains aggregate interference below the protected entity's protection threshold,

whether it is calculated at the location of the protected entity, or on grid points within a pre-defined protection area. This section only provides the template for test cases that will be referenced in subsequent sections per the protected entity type.

9.3.5 ESC protection (Possible option)

ESC protection testing during Fairspectrum ICD depends on the availability of certified ESCs and ESC indicated protection requirements. This section provides the target of testing scenario for SAS to grant CBSDs only when they do not interfere with its hosted ESC sensors. The scope of this test is to verify that the SAS continuously maintains aggregate interference below the ESC sensors' protection threshold. In addition, a test case is included to verify ESC sensor protection when multiple SASs are present. ESC sensors in all cases are active.

9.3.6 PPA protection

This section provides the target of testing scenario for testing that Fairspectrum SAS can protect one or more pre-defined PPA zones.

9.3.7 GWPZ protection

This section provides the target of testing scenario for testing that Fairspectrum SAS can protect one or more pre-defined GWPZ.

9.3.8 FSS protection

This section provides the target of testing scenario for SAS to grant CBSDs to protect FSS earth station. The scope of this section is to verify that SAS would not authorize CBSD Grants when they interfere with FSS. In addition, test cases are included to verify FSS protection when multiple SASs are present. It is assumed that all the necessary information regarding FSS sites are available and can be injected to the Fairspectrum SAS.

9.3.9 Federal incumbent protection

This section provides the target of testing scenario to test that SAS meets established criteria for the protection of federal incumbent dynamic protection areas (DPAs). It tests the response of Fairspectrum

SAS to new Grant Requests, as well as the ability of Fairspectrum SAS to manage the aggregate interference of existing authorized CBSD Grants when DPAs are activated. Possibly, it also tests the response of Fairspectrum SAS to loss of connectivity with the ESC.

9.3.10 Incumbent protection - Multi constraint protection

This section provides the target of testing scenario to test that Fairspectrum SAS meets established criteria for interference protection with multiple constraints, including FSS, GWPZ, PPA, ESC sensor, and DPA. It tests the response of Fairspectrum SAS to Grant Requests subject to one or more of these constraints.

9.3.11 SAS Federal government database update

This section provides the target of testing scenario of the SAS operation to access external database managed by Federal Government, pull the data, and to update its database accordingly.

9.3.12 SAS WINNF Database update

This section provides the target of testing scenario for successful execution and completion of the SAS operation to verify that SAS UUT can retrieve and update its database with shared PAL and CPI Databases.

9.3.13 International border protection

This section provides the target of testing scenario to verify that SAS properly handles Grants for CBSDs located near the International Borders of the US. While Part96 has not clearly outlined the requirements of the International border protection, WInnForum has defined the criteria for SAS to approve the operation of CBSDs near the border.

9.3.14 Quiet Zone protection

This section provides the target of testing scenario to verify that SAS protects designated Quiet Zones. The CBSD shall not be authorized to transmit in the Quiet Zones, without appropriate coordination.

9.4 Channel allocation

This section provides the target of testing scenario of channel allocation. Fairspectrum determines the available and suitable frequency ranges for CBSDs by utilizing a combination of Registration, Spectrum Inquiry, Grant, and Heartbeat procedures of WINNF-TS-00169 or its latest version. In the Registration procedure, CBSD delivers its location and configuration. In Spectrum Inquiry, CBSD optionally requests the range of available operation parameters. In Grant, CBSD requests a specific set of operational parameter to be used. In Heartbeat, a successful Grant is authorized and the authorization is maintained. Heartbeat procedure is maintained during the transmission of CBSD. Any changes in protection, which limit the availability of the CBSD grant, are signalled from SAS to CBSD with Heartbeat Response.

9.5 Coordinated incumbent protection

This section provides the target of testing scenario of coordinated incumbent protection. Fairspectrum supports the Coordination events according to WINNF-TS-0096[35].

9.6 Coordinated PAL protection

This section provides the target of testing scenario of coordinated PAL protection. Fairspectrum supports the Coordination events according to WINNF-TS-0096.

10 Generated data

Each ICD Proposal must include … descriptions of the type of data it intends to generate during ICD, and a discussion of how this data will be provided in its final report.

Fairspectrum collects user related data, user device data. Fairspectrum keeps access authorization logs. Fairspectrum logs the system software updates and issues related to the SAS software implementation. Fairspectrum logs the dataset updates from all information sources, with the following exception: Fairspectrum does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any

[35] WINNF-TS-0096. Spectrum Access System (SAS) - SAS Interface Technical Specification. Apr 24, 2018.

federal system that is not required by this part to effectively operate the SAS.

Fairspectrum creates logs of SAS-CBSD communication and SAS-SAS communication. Fairspectrum populates and maintains PAL database in cooperation with other SAS Administrators. Fairspectrum maintains interference reports. Fairspectrum records initial value and the results of the test cases described in section 9 Description of testing scenarios.

In the final report, Fairspectrum provides examples of data in the form that it does not reveal any privacy information or federal use of spectrum. Fairspectrum provides a statistical or written description of each generated data type. Fairspectrum establishes and follows protocols to respond to instructions from FCC, the President of the United States, or another designated Federal government entity, issued pursuant to 47 U.S.C. 606[36].

Fairspectrum logs all access to and use of SAS in a format which can with a reasonable effort be transferred to another database platform. Fairspectrum supports WINNF-TS-0096[37] or its latest version and ensures that the required business processes are in place for SAS-to-SAS communication. Fairspectrum SAS service contains a web user interface including a map functionality, which can be used to provide non-federal, non-proprietary information to general public, among other things. Fairspectrum provides FCC with both machine-to-machine and human user interface to verify various functionalities of the SAS service.

11 Access to the SAS and data

ICD Proposals must also describe the method by which staff involved with the review of ICD Proposals will be provided with access to the SAS and data generated by the SAS during ICD.

Fairspectrum provides a web-based user interface for FCC. Through the interface FCC is able to check the incumbent data, registered CBSDs, log data of SAS service use, and current spectrum allocations. The queries can be narrowed based on location, time, frequency, and IDs. FCC interface allows to

[36] 47 U.S.C. 606 Title 47. Telegraphs, telephones, and radiotelegraphs. Chapter 5. Wire or radio communication. Subchapter VI. Miscellaneous provisions. Sec. 606. War powers of president.

[37] WINNF-TS-0096. Spectrum Access System (SAS) - SAS Interface Technical Specification. Apr 24, 2018.

block and release selectable channels from GAA and PAL use on a restricted area for a defined time. Commission can set and clear a blacklist based on devices, device owners, or licenses.

Regular backups are created also for the FCC data on the Fairspectrum SAS server, so that the previous version of the data can be restored in the case of errors. The Fairspectrum SAS filesystem is encrypted. The servers and data storages are located in Amazon AWS cloud service in the US. The data is stored as original files in the filesystem, in tables in the database, and in backup files. Temporarily, small and specific parts of the data may be stored for debugging, error solving, or development purposes on the hard disks of the developers and system administrators.

Fairspectrum SAS operates without any connectivity to any military or other sensitive federal database or system, except as otherwise required by this part; and it does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the SAS.

12 Technical verification, and

Each ICD Proposal must also describe the technical data that the SAS Administrator will provide to verify the proper operation of its SAS and discuss how it will provide a means of verifying the technical data generated during this real world deployment and the subsequent test results.

As described in section 10 Generated data among other things, Fairspectrum keeps access authorization logs. Fairspectrum logs the system software updates and issues related to the SAS software implementation. Fairspectrum logs the dataset updates from all information sources with the following exception: Fairspectrum does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the SAS. Fairspectrum creates logs of SAS-CBSD communication and SAS-SAS communication.Fairspectrum maintains interference reports. Fairspectrum records initial value and the results of the test cases described in section 9 Description of testing scenarios.

As described in section 11 Access to the SAS and data, Fairspectrum provides a web-based user interface for FCC. Through the interface FCC is able to check the incumbent data, registered CBSDs, log data of SAS service use, and current spectrum allocations.

As described in section 13 Description of report after the ICD period, Fairspectrum creates a report after the ICD period, which among other things, contains technical verification in written format and is based on the data generated during the ICD period.

13 Description of report after the ICD period

Finally, each ICD Proposal must also include a detailed description of the report that the SAS Administrator plans to produce at the conclusion of its ICD period to demonstrate compliance with the Commission's rules and the requirements set forth in this Public Notice.

Fairspectrum report after the ICD period describes the II Model of CBRS spectrum access, III ICD network setup, IV Testing scenarios and results, V Experimental verification of Fairspectrum SAS in ICD, and VI Conclusions. The more detailed planned outline of the report can be found below.

Table 1. Outline of planned report after the ICD period

I Introduction	
II Model of CBRS spectrum access	
A Spectrum sharing model	Fig System architecture
B Procedures	Fig Flow chart of procedures
C Protocols implementing the procedures	Fig Protocol picture
III ICD network setup	Fig Demonstration system
A Operator network	Fig Operator network picture
B Incumbents in the area	Fig Incumbents
C Other CBSDs	Fig Other CBSDs

D Fairspectrum SAS — Fig Fairspectrum SAS achitecture

E FCC User Interface — Fig FCC User interface

F Operator User interface — Fig Operator User interface

G Spectrum allocation algorithm — Fig Algorithm

IV Testing scenarios and results

A SAS-CBSD Interface tests — Fig Testing scenario A

A.1 CBSD Registration

A.2 CBSD Spectrum Inquiry

A.3 CBSD Spectrum Grant

A.4 CBSD Heartbeat

A.5 CBSD Measurement report

A.6 CBSD Spectrum Relinquish

A.7 CBSD Deregistration

A.8 CBSD Device Security Validation

A.9 CBSD Domain Proxy Security Validation

B SAS-SAS Interface tests — Fig Testing scenario B

B.1 SAS-SAS Security, Authentication, and Encryption Protocols

B.2 SAS-SAS Full Activity Dump Message

C SAS Functional tests — Fig Testing scenario C

C.1 Exclusion Zone Enforcement

C.2 Propagation model and antenna gain

C.3 PPA creation

C.4 Aggregate interference protection - Single Protected Entity

C.6 PPA protection

C.7 GWPZ protection

C.8 FSS protection

C.9 Federal incumbent protection

C.10 Incumbent protection - Multi constraint protection

C.11 SAS Federal government database update

C.12 SAS WINNF Database update

C.13 International border protection

C.14 Quiet Zone protection

D Channel allocation	Fig Testing scenario D
E Coordinated incumbent protection	Fig Testing scenario E
F Coordinated PAL protection	Fig Testing scenario F
G Data collection	Fig Data collection

V Experimental verification of Fairspectrum SAS in ICD

A User registration process

B SAS-CBSD Communications

C Professional Installation

D SAS-SAS Interoperability

F SAS Utilization of Commission Databases

G DPA Protection

H Incumbent Protection Implementation

I Interference Reports and Mitigation

J Access to the SAS and data

K Technical verification

L Results from testing scenarios

M Data analysis

VI Conclusions

References

Wireless Innovation Forum, Spectrum Sharing Committee (SSC), Release 1
WINNF-TS-0016[38]
WINNF-TS-0022[39]
WINNF-TS-0061[40]
WINNF-TS-0065[41]
WINNF-TS-0071[42]
WINNF-TS-0096[43]
WINNF-TS-0112[44]
WINNF-TS-0122[45]
WINNF-TS-0245[46]
WINNF-TS-0247[47]

Code of Federal Regulations

Title 47	Code of Federal Regulations, Telecommunications, available at: www.ecfr.gov.
Title 47, Part 96	Citizens Broadband Radio Service. Available at http://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.96&rgn=div5.
47 C.F.R. § 2.106	Table of frequency allocations.
47 C.F.R. § 96.17	Protection of existing fixed satellite service (FSS) earth stations in the 3600-3700 MHz Band and 3700-4200 MHz Band.
47 C.F.R. § 96.25	Priority Access Licenses.
47 C.F.R. § 96.39	Citizens Broadband Radio Service Device (CBSD) general requirements.
47 C.F.R. § 96.41	General radio requirements.
47 C.F.R. § 96.43	Additional requirements for category A CBSDs.
47 C.F.R. § 96.45	Additional requirements for category B CBSDs.
47 C.F.R. § 96.49	Equipment authorization.
47 C.F.R.§ 96.55	Information gathering and retention.

[38] WINNF-TS-0016. Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD). V1.2.1. Jan 3, 2018.
[39] WINNF-TS-0022. CBRS Certificate Policy Specification. V1.1.2. Feb 6, 2018.
[40] WINNF-TS-0061. SAS as Unit Under Test (UUT). V1.2.0. Jun 6, 2018.
[41] WINNF-TS-0065. CBRS Communications Security Technical Specification. V1.1.0. Jul 26, 2017.
[42] WINNF-TS-0071. CBRS Operational Security. V1.0.0. Jul 26, 2017.
[43] WINNF-TS-0096. Spectrum Access System (SAS) - SAS Interface Technical Specification. Apr 24, 2018.
[44] WINNF-TS-0112. Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band. V1.5.0. May 1, 2018.
[45] WINNF-TS-0122. CBSD/DP as Unit Under Test (UUT). V1.0.0. Dec 19, 2017.
[46] WINNF-TS-0245. Priority Access License (PAL) Database Technical Specification. V1.0.0. Jul 26, 2017.
[47] WINNF-TS-0247. CBRS Certified Professional Installer Accreditation Technical Specification. V1.0.0. Oct 16, 2017.

Code of Laws of the United States of America

47 U.S.C. 606 Title 47. Telegraphs, telephones, and radiotelegraphs. Chapter 5. Wire or radio communication. Subchapter VI. Miscellaneous provisions. Sec. 606. War powers of president.

Federal Communications Commission

FCC 15-47 Federal Communications Commission, "Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band,"GN Docket 12-354, FCC 15-47, Report and Order and Second Notice of Proposed Rulemaking, Released April 21, 2015, available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-47A1_Rcd.pdf.

FCC EAS FCC Equipment Authorization System. Available at https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

National Telecommunications and Information Administration

NTIA 3550-3650. NTIA. Spectrum Management. 3550-3650 MHz. Available at https://www.ntia.doc.gov/category/3550-3650-mhz.

ITM NTIA – ITS Irregular Terrain Model (ITM) (Longley-Rice) (20MHz-20 GHz): http://www.its.bldrdoc.gov/resources/radio-propagation-software/itm/itm.aspx

3.5 GHz EZ NTIA. 3.5 GHz Exclusion Zone Analyses and Methodology Available at https://www.ntia.doc.gov/report/2015/35-ghz-exclusion-zone-analyses-and-methodology

IETF

RFC-5280. Internet X.509 Public Key Infrastructure Certificate and Certification Revocation List (CRL) Profile. Available at https://www.ietf.org/rfc/rfc5280.txt.

RFC-5246. The Transport Layer Security (TLS) Protocol Version 1.2. Available at https://www.ietf.org/rfc/rfc5246.txt.

RFC-7159. The JavaScript Object Notation (JSON) Data Interchange Format.

ISO/IEC

ISO/IEC 27001:2013(en) Information technology. Security techniques. Information security management systems. Requirements.

ISO/IEC 27002:2013(en) Information technology. Security techniques. Code of practice for information security controls.

Other

ITS Institute for Telecommunication Sciences. Irregular Terrain Model (ITM) (Longley-Rice) (20 MHz - 20 GHz). Available at https://www.its.bldrdoc.gov/resources/radio-propagation-software/itm/itm.aspx.

Census Tract	United States. Census Bureau. Topologically Integrated Geographic Encoding and Referencing. https://www.census.gov/geo/maps-data/data/tiger.html
OpenSSRF	Open source Standard Spectrum Resource Format. See,http://openssrf.org/.

Yours respectfully,

Heikki Kokkinen
CEO, Fairspectrum LLC
265 Franklin Street, Suite 1702,
Boston, MA 02110, USA
617-963-3585
heikki.kokkinen@fairspectrumllc.com

E. Barlow Keener
Counsel for Fairspectrum LLC
bk@keenerlawgroup.com
d. 617-671-1202